Projected Subcodes of the Second Order Binary Reed-Muller Code

Matthieu Legeay

IRMAR, University of Rennes 1, France

CBC 2012

Plan

Motivation

- Reed-Muller codes have efficient decoding algorithms

Motivation

- Reed-Muller codes have efficient decoding algorithms

$\Rightarrow$ No algorithm reaches the lower bound on the minimum distance decoding capability

Motivation

- Reed-Muller codes have efficient decoding algorithms

$\Rightarrow$ No algorithm reaches the lower bound on the minimum distance decoding capability

- Other algorithms using algebraic properties practically correct more errors

Motivation

- Reed-Muller codes have efficient decoding algorithms

$\Rightarrow$ No algorithm reaches the lower bound on the minimum distance decoding capability

- Other algorithms using algebraic properties practically correct more errors

$\Rightarrow$ The complexity of the decoder is quadratic in the code length

Principle

Take $y = c + e$ and compute :

$$\sum_i \lambda_i \sigma_i(y) = \sum_i \lambda_i \sigma_i(c) + \sum_i \lambda_i \sigma_i(e)$$

where $(\sigma_i)_i \in Perm(C)$ and $(\lambda_i)_i \in \mathbb{F}_2$.

Principle

Take $y = c + e$ and compute :

$$\sum_i \lambda_i \sigma_i(y) = \sum_i \lambda_i \sigma_i(c) + \sum_i \lambda_i \sigma_i(e)$$

where $(\sigma_i)_i \in Perm(C)$ and $(\lambda_i)_i \in \mathbb{F}_2$.

$\Rightarrow c' = \sum_i \lambda_i \sigma_i(c)$ lives in a subcode C_{ad} of C, with $k_{ad} \leq k$.

Principle

Take $y = c + e$ and compute :

$$\sum_i \lambda_i \sigma_i(y) = \sum_i \lambda_i \sigma_i(c) + \sum_i \lambda_i \sigma_i(e)$$

where $(\sigma_i)_i \in Perm(C)$ and $(\lambda_i)_i \in \mathbb{F}_2$.

$\Rightarrow c' = \sum_i \lambda_i \sigma_i(c)$ lives in a subcode C_{ad} of C, with $k_{ad} \leq k$.

$\Rightarrow e' = \sum_i \lambda_i \sigma_i(e)$ is an error vector, $wt(e') \leq \lambda t$.

Recalls

r-order Reed-Muller codes

Let $0 \leq r \leq m$, $n = 2^m$ and $(\alpha_1, \ldots, \alpha_n) \in (\mathbb{F}_2^m)^n$.

$$\mathcal{R}(r, m) = \{(f(\alpha_1), \ldots, f(\alpha_n)) \in \mathbb{F}_2^n\}$$

with $f(x_1, \ldots, x_m)$ a binary multivariate polynomial of degree $\leq r$.

Recalls

r-order Reed-Muller codes

Let $0 \leq r \leq m$, $n = 2^m$ and $(\alpha_1, \ldots, \alpha_n) \in (\mathbb{F}_2^m)^n$.

$$\mathcal{R}(r, m) = \{(f(\alpha_1), \ldots, f(\alpha_n)) \in \mathbb{F}_2^n\}$$

with $f(x_1, \ldots, x_m)$ a binary multivariate polynomial of degree $\leq r$.

- $\mathcal{R}(r, m)$ is a $[n = 2^m, k = \sum_{i=0}^{r} \binom{m}{i}, d = 2^{m-r}]$ code.

Recalls

r-order Reed-Muller codes

Let $0 \leq r \leq m$, $n = 2^m$ and $(\alpha_1, \ldots, \alpha_n) \in (\mathbb{F}_2^m)^n$.

$$\mathcal{R}(r, m) = \{(f(\alpha_1), \ldots, f(\alpha_n)) \in \mathbb{F}_2^n\}$$

with $f(x_1, \ldots, x_m)$ a binary multivariate polynomial of degree $\leq r$.

- $\mathcal{R}(r, m)$ is a $[n = 2^m, k = \sum_{i=0}^{r} \binom{m}{i}, d = 2^{m-r}]$ code.
- $\mathcal{R}(0, m)$ is the repetition code.

Recalls

r-order Reed-Muller codes

Let $0 \leq r \leq m$, $n = 2^m$ and $(\alpha_1, \ldots, \alpha_n) \in (\mathbb{F}_2^m)^n$.

$$\mathcal{R}(r, m) = \{(f(\alpha_1), \ldots, f(\alpha_n)) \in \mathbb{F}_2^n\}$$

with $f(x_1, \ldots, x_m)$ a binary multivariate polynomial of degree $\leq r$.

- $\mathcal{R}(r, m)$ is a $[n = 2^m, k = \sum_{i=0}^{r} \binom{m}{i}, d = 2^{m-r}]$ code.
- $\mathcal{R}(0, m)$ is the repetition code.
- $\mathcal{R}(m, m)$ is all the space $\mathbb{F}_2^n$.

Permutation group

Theorem

$$\begin{aligned} Perm(\mathcal{R}(r,m)) &= GA_m(\mathbb{F}_2) \\ &= \mathcal{T} \rtimes GL_m(\mathbb{F}_2) \end{aligned}$$

Permutation group

Theorem

$$\begin{aligned} Perm(\mathcal{R}(r,m)) &= GA_m(\mathbb{F}_2) \\ &= \mathcal{T} \rtimes GL_m(\mathbb{F}_2) \end{aligned}$$

- $\mathcal{T} = \left\{ T_\alpha : \begin{array}{ccc} \mathbb{F}_2^m & \rightarrow & \mathbb{F}_2^m \\ x & \mapsto & x+\alpha \end{array} \right\}, \alpha \in \mathbb{F}_2^m$

$$T_\alpha \cdot f\ (x) \overset{def}{=} f(T_\alpha(x)) = f(x+\alpha)$$

Permutation group

Theorem

$$\begin{aligned} Perm(\mathcal{R}(r,m)) &= GA_m(\mathbb{F}_2) \\ &= \mathcal{T} \rtimes GL_m(\mathbb{F}_2) \end{aligned}$$

- $\mathcal{T} = \left\{ T_\alpha : \begin{array}{ccc} \mathbb{F}_2^m & \rightarrow & \mathbb{F}_2^m \\ x & \mapsto & x+\alpha \end{array} \right\}, \alpha \in \mathbb{F}_2^m$

$$T_\alpha \cdot f\ (x) \stackrel{def}{=} f(T_\alpha(x)) = f(x+\alpha)$$

- $GL_m(\mathbb{F}_2) = \{$ non-singular binary matrices G of size $m \times m\}$

$$G \cdot f\ (x) \stackrel{def}{=} f(G.x)$$

With $\mathcal{T}$

Proposition 1

$(Id + T_\alpha) \cdot \mathcal{R}(2, m) \overset{def}{=} \{f + T_\alpha \cdot f | f \in \mathcal{R}(2, m)\}$ is a subcode of $\mathcal{R}(2, m)$.

With $\mathcal{T}$

Proposition 1

$(Id + T_\alpha) \cdot \mathcal{R}(2, m) \overset{def}{=} \{f + T_\alpha \cdot f | f \in \mathcal{R}(2, m)\}$ is a subcode of $\mathcal{R}(2, m)$.

Proposition 2

$(Id + T_\alpha) \cdot \mathcal{R}(2, m)$ is isomorphic to $\mathcal{R}(1, m - 1)$.

With $\mathcal{T}$

Proposition 1

$(Id + T_\alpha) \cdot \mathcal{R}(2, m) \stackrel{def}{=} \{f + T_\alpha \cdot f | f \in \mathcal{R}(2, m)\}$ is a subcode of $\mathcal{R}(2, m)$.

Proposition 2

$(Id + T_\alpha) \cdot \mathcal{R}(2, m)$ is isomorphic to $\mathcal{R}(1, m-1)$.

Idea for proof...

1. $(f + T_\alpha \cdot f)$ is an affine function $x \Rightarrow r' = 1$
2. $(f + T_\alpha \cdot f)(x + \alpha) = (f + T_\alpha \cdot f)(x) \Rightarrow m' = m - 1$

With $GL_m(\mathbb{F}_2)$

Proposition 1

$(Id + G) \cdot \mathcal{R}(2, m) \stackrel{def}{=} \{f + G \cdot f | f \in \mathcal{R}(2, m)\}$ is a subcode of $\mathcal{R}(2, m)$.

With $GL_m(\mathbb{F}_2)$

Proposition 1

$(Id + G) \cdot \mathcal{R}(2, m) \stackrel{def}{=} \{f + G \cdot f | f \in \mathcal{R}(2, m)\}$ is a subcode of $\mathcal{R}(2, m)$.

What are the properties of this subcode ?
Length ? Dimension ? Minimum Distance ?

With $GL_m(\mathbb{F}_2)$

Proposition 1

$(Id + G) \cdot \mathcal{R}(2, m) \stackrel{def}{=} \{f + G \cdot f | f \in \mathcal{R}(2, m)\}$ is a subcode of $\mathcal{R}(2, m)$.

What are the properties of this subcode ?
Length ? Dimension ? Minimum Distance ?

$\Rightarrow$ Hard to answer in the general case.

With $GL_m(\mathbb{F}_2)$

- By writing $f(x) = x^t F x + a_f$, with F upper triangular,

$$(f + G \cdot f)(x) = x^t(F + G^t F G)x$$

$\rightsquigarrow \mathcal{P}_G : \begin{array}{ccc} \mathcal{M}_m(\mathbb{F}_2) & \to & \mathcal{M}_m(\mathbb{F}_2) \\ F & \mapsto & F + G^t F G \end{array}$ does not keep upper-triangularity.

With $GL_m(\mathbb{F}_2)$

- By writing $f(x) = x^t Fx + a_f$, with F upper triangular,

$$(f + G \cdot f)(x) = x^t(F + G^t FG)x$$

$\rightsquigarrow \mathcal{P}_G : \begin{array}{ccc} \mathcal{M}_m(\mathbb{F}_2) & \to & \mathcal{M}_m(\mathbb{F}_2) \\ F & \mapsto & F + G^t FG \end{array}$ does not keep upper-triangularity.

- Rewrite $G = Id + E$, hence

$$(f + G \cdot f)(x) = x^t(E^t F + FE + E^t FE)x$$

$$\rightsquigarrow \mathcal{P}_E : \begin{array}{ccc} \mathcal{M}_m(\mathbb{F}_2) & \to & \mathcal{M}_m(\mathbb{F}_2) \\ F & \mapsto & E^t F + FE + E^t FE \end{array}$$

With $GL_m(\mathbb{F}_2)$

- By writing $f(x) = x^t F x + a_f$, with F upper triangular,

$$(f + G \cdot f)(x) = x^t (F + G^t F G) x$$

$\rightsquigarrow \mathcal{P}_G : \begin{array}{ccc} \mathcal{M}_m(\mathbb{F}_2) & \to & \mathcal{M}_m(\mathbb{F}_2) \\ F & \mapsto & F + G^t F G \end{array}$ does not keep upper-triangularity.

- Rewrite $G = Id + E$, hence

$$(f + G \cdot f)(x) = x^t (E^t F + FE + E^t FE) x$$

$$\rightsquigarrow \mathcal{P}_E : \begin{array}{ccc} \mathcal{M}_m(\mathbb{F}_2) & \to & \mathcal{M}_m(\mathbb{F}_2) \\ F & \mapsto & E^t F + FE + E^t FE \end{array}$$

$\Rightarrow$ **Rank of** E

Result on length

Proposition 2

$(Id + G) \cdot \mathcal{R}(2, m)$ is isomorphic to a subcode of length $n - 2^{m-r}$

Result on length

Proposition 2

$(Id + G) \cdot \mathcal{R}(2, m)$ is isomorphic to a subcode of length $n - 2^{m-r}$

- If $r = 1$, $n' = 2^{m-1}$
  we find again that the subcode is isomorphic to $\mathcal{R}(1, m-1)$.
- If $r = 2$, $n' = 2^m - 2^{m-2}$...

Result on length

Proposition 2

$(Id + G) \cdot \mathcal{R}(2, m)$ is isomorphic to a subcode of length $n - 2^{m-r}$

- If $r = 1$, $n' = 2^{m-1}$
  we find again that the subcode is isomorphic to $\mathcal{R}(1, m-1)$.
- If $r = 2$, $n' = 2^m - 2^{m-2}$...

$\Rightarrow$ We can do better...
Some columns are equal in practice.

Result on dimension

Proposition 3

$(Id + G) \cdot \mathcal{R}(2, m)$ has dimension $k' \leq 4r(m - r) + 1$

Idea for proof...

1. $\mathrm{Rank}(E^t F + FE + E^t FE) \leq 2r$
2. $\mathcal{N}(m, r) = \sum_{j=0}^{r} \prod_{i=0}^{j-1} \frac{(2^m - 2^i)(2^m - 2^i)}{2^j - 2^i} \leq 2^{(2m-r)r+1)}$

Result on dimension

Proposition 3

$(Id + G) \cdot \mathcal{R}(2, m)$ has dimension $k' \leq 4r(m-r)+1$

Idea for proof...

1. $\mathrm{Rank}(E^tF + FE + E^tFE) \leq 2r$
2. $\mathcal{N}(m,r) = \sum_{j=0}^{r} \prod_{i=0}^{j-1} \frac{(2^m-2^i)(2^m-2^i)}{2^j-2^i} \leq 2^{(2m-r)r+1)}$

- If $r=1$, $k' \leq 4(m-1)+1$
- If $r=2$, $k' \leq 8(m-2)+1$...

Result on dimension

Proposition 3

$(Id + G) \cdot \mathcal{R}(2, m)$ has dimension $k' \leq 4r(m-r)+1$

Idea for proof...

1. $\text{Rank}(E^t F + FE + E^t FE) \leq 2r$
2. $\mathcal{N}(m, r) = \sum_{j=0}^{r} \prod_{i=0}^{j-1} \frac{(2^m - 2^i)(2^m - 2^i)}{2^j - 2^i} \leq 2^{(2m-r)r+1)}$

- If $r = 1$, $k' \leq 4(m-1)+1$
- If $r = 2$, $k' \leq 8(m-2)+1$...

$\Rightarrow$ This bound is only intersting for small values of r ($r \leq 0.15m$).

Result on dimension

With E of shape $E(\mathbf{e}_1, \ldots, \mathbf{e}_{m-1}) = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \mathbf{e}_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{e}_{m-1} & & & 0 \end{pmatrix}$

where $\mathbf{e}_i$ is a binary vector of length i

Result on dimension

With E of shape $E(\mathbf{e}_1, \ldots, \mathbf{e}_{m-1}) = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \mathbf{e}_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{e}_{m-1} & & & 0 \end{pmatrix}$

where $\mathbf{e}_i$ is a binary vector of length i

Proposition 4

$(Id + G) \cdot \mathcal{R}(2, m)$ has dimension $k' \leq \sum_{i=0}^{r-1}(m-i) = rm - \frac{r(r-1)}{2}$

Result on dimension

With E of shape $E(\mathbf{e}_1, \ldots, \mathbf{e}_{m-1}) = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \mathbf{e}_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{e}_{m-1} & & & 0 \end{pmatrix}$

where $\mathbf{e}_i$ is a binary vector of length i

Proposition 4

$(Id + G) \cdot \mathcal{R}(2, m)$ has dimension $k' \leq \sum_{i=0}^{r-1}(m - i) = rm - \frac{r(r-1)}{2}$

$\Rightarrow$ This bound is never reached in practice...

Result on minimum distance

Remark

$(Id + G) \cdot \mathcal{R}(2, m)$ has minimum distance $d' \geq d = 2^{m-2}$

Result on minimum distance

Remark

$(Id + G) \cdot \mathcal{R}(2, m)$ has minimum distance $d' \geq d = 2^{m-2}$

$\Rightarrow$ In practice $d' = d = 2^{m-2}$...

Examples (1/2)

$$G = Id + E = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ g_1 & 1 & 0 & 0 & 0 \\ 0 & g_2 & 1 & 0 & 0 \\ 0 & 0 & g_3 & 1 & 0 \\ 0 & 0 & 0 & g_4 & 1 \end{pmatrix}$$

Examples (1/2)

$$G = Id + E = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ g_1 & 1 & 0 & 0 & 0 \\ 0 & g_2 & 1 & 0 & 0 \\ 0 & 0 & g_3 & 1 & 0 \\ 0 & 0 & 0 & g_4 & 1 \end{pmatrix}$$

- G_1 : $g_1 = 1$ and $g_2 = g_3 = g_4 = 0$
  $(Id + G_1) \cdot \mathcal{R}(2,5)$ is a $[32,4,8]$ subcode, isomorphic to $\mathcal{R}(1,3)$

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Examples (2/2)

- $G_2 : g_1 = g_2 = 1$ and $g_3 = g_4 = 0$
  $(Id + G_2) \cdot \mathcal{R}(2,5)$ is a $[32, 8, 8]$ subcode.
  We have $k' = 2m - 2 \leq 2m - 1$.

Examples (2/2)

- $G_2 : g_1 = g_2 = 1$ and $g_3 = g_4 = 0$
  $(Id + G_2) \cdot \mathcal{R}(2,5)$ is a $[32, 8, 8]$ subcode.
  We have $k' = 2m - 2 \leq 2m - 1$.

- $G_3 : g_1 = g_2 = g_3 = 1$ and $g_4 = 0$
  $(Id + G_3) \cdot \mathcal{R}(2,5)$ is a $[32, 10, 8]$ subcode.
  We have $k' = 3m - 5 \leq 3m - 3$.

Examples (2/2)

- $G_2 : g_1 = g_2 = 1$ and $g_3 = g_4 = 0$
  $(Id + G_2) \cdot \mathcal{R}(2,5)$ is a $[32, 8, 8]$ subcode.
  We have $k' = 2m - 2 \leq 2m - 1$.

- $G_3 : g_1 = g_2 = g_3 = 1$ and $g_4 = 0$
  $(Id + G_3) \cdot \mathcal{R}(2,5)$ is a $[32, 10, 8]$ subcode.
  We have $k' = 3m - 5 \leq 3m - 3$.

- $G_4 : g_1 = g_2 = g_3 = g_4 = 1$
  $(Id + G_4) \cdot \mathcal{R}(2,5)$ is a $[32, 12, 8]$ subcode.
  We have $k' = 4m - 8 \leq 4m - 6$.

Conclusion

$\Rightarrow$ We have constructed new subcodes from $\mathcal{R}(2, m)$

$\Rightarrow$ We have a bound on the dimension of the projected codes, and in some cases we can tighten it.

Conclusion

$\Rightarrow$ We have constructed new subcodes from $\mathcal{R}(2, m)$

$\Rightarrow$ We have a bound on the dimension of the projected codes, and in some cases we can tighten it.

- To have better results for all possible matrices E.
- To understand the improvements we have in practice.
- To apply this principle with a view to decoding.

Thank You for your attention !